SURVEILLANCE POLICY

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Investigatory Powers Act 2016

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE REVISED HOME OFFICE CODES OF PRACTICE: "COVERT SURVEILLANCE AND PROPERTY INTERFERENCE" AND "COVERT HUMAN INTELLIGENCE SOURCES" (AUGUST 2018) AND ANY GUIDANCE ISSUED BY THE INVESTIGATORY POWERS COMMISSIONER'S OFFICE

CONTENTS **Page**

1 BACKGROUND

1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.

1.2 Article 8 of the Convention reads as follows: -

"Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others."

1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person's right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.

1.4 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework whereby certain surveillance activities can be authorised and conducted compatibly with Article 8 by public bodies. RIPA is also supplemented by the relevant provisions of the Investigatory Powers Act 2016.

1.5 Officers of New Forest District Council ("the Council") may seek authorisation under RIPA to engage in the following types of surveillance: -

- Directed surveillance
- Use of a Covert Human Intelligence Source

1.6 These surveillance techniques can **only** be authorised under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime**, or (in some cases) for the **prevention of disorder**. Since **1 November 2012**, it is **only** possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months' imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.

1.7 The Council can only authorise surveillance under RIPA in connection with the performance of the specific public functions which it carries out. It cannot use RIPA to authorise surveillance in connection with the ordinary functions (e.g., employment issues) which are carried out by all public authorities.

1.8 This Surveillance Policy explains what is involved in each of these two types of surveillance. The policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any such surveillance is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA.

1.9 All Investigating Officers and Authorising Officers should be familiar with RIPA, this Surveillance Policy, the Codes of Practice issued by the Home Office relating to the Use of Covert Human Intelligence Sources and Covert Surveillance and Property

Interference, and the Procedures and Guidance issued by the Investigatory Powers Commissioner's Office

2 DEFINITIONS:

2.1 Confidential Information

This includes:

- Matters subject to legal privilege: Information relating to communications between a professional legal advisor and their client for the purposes of giving advice, in contemplation of legal proceedings or relating to legal proceedings.
- Confidential personal information: Information which relates to the physical or mental health, or spiritual counselling of a person (living or dead) who can be identified from it. For example, information about medical consultations/medical records.
- Confidential constituent information: Information relating to communications between a Member of Parliament and constituent in respect of constituency matters.
- Confidential journalistic information

2.2 Collateral Intrusion

Collateral Intrusion is the likely effect of the use of surveillance on the private and family life of persons who are not the intended subjects of the activity.

2.3 Surveillance

Surveillance includes

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- recording anything monitored, observed or listened to in the course of surveillance.
- surveillance by, or with, the assistance of a surveillance device.

Surveillance can be **overt** or **covert**.

2.4 Overt Surveillance

Overt surveillance is surveillance which is not secretive or hidden. It includes surveillance where the subject has been told it will happen.

2.5 **Covert Surveillance**

Covert surveillance is surveillance carried out in a manner calculated to ensure that subjects of it are unaware that it is or may be taking place.

2.6 **Directed Surveillance**

Directed surveillance is **covert** but **not intrusive** and is undertaken:

- For the purposes of a specific investigation or a specific operation
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) and
- Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance

2.7 **Intrusive surveillance**

Intrusive Surveillance occurs when surveillance:

- is covert;
- relates to residential premises and/or private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Intrusive surveillance cannot be carried out or approved by the Council.

2.8 **The conduct and use of covert human intelligence sources (CHIS)**

The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person or

To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

3 DIRECTED SURVEILLANCE

3.1 This paragraph should be read in conjunction with the Revised Home Office Code of Practice “Covert Surveillance and Property Interference” which can be found at https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

3.2 Directed surveillance is surveillance which meets **all** of the following criteria:

i. It is covert, but not intrusive surveillance

Surveillance will be covert if it is carried out in a way calculated to ensure that the subject of the surveillance is unaware that it is taking place.

The Council **cannot** engage in intrusive surveillance.

ii. It is conducted for the purposes of a specific investigation or operation

iii. It is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation)

"Private information" includes any information relating to a person's private or family life, including their relationships with others, their family, and professional or business relationships.

For more information about what constitutes "private information", see paragraph 5 below.

iv. It is conducted otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonable for an authorisation under RIPA to be sought.

For example, if an officer happens to spot an offence taking place, they may stop and take photographs as evidence of that offence, without requiring prior authorisation under RIPA.

3.3 Any officer intending to conduct directed surveillance must seek prior authorisation of that surveillance under RIPA (see paragraphs 8,9 & 10 below, regarding applications and authorisations).

3.4 Since **1 November 2012**, it is **only** possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months' imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.

3.5 **Examples**

3.5.1 Since 1 November 2012, it is no longer possible to authorise directed surveillance under RIPA for the following offences:

- Dog fouling
- Littering
- Planning offences
- Noise abatement notices

As the courts **cannot** impose a maximum term of at least six months' imprisonment.

3.5.2 It is possible to authorise directed surveillance under RIPA for some offences under the following categories:

- Fly tipping
- Benefit fraud
- Trading standards offences
- Financial offences
- Dangerous dogs
- Listed building offences

As the courts **can** impose a maximum term of at least six months' imprisonment.

3.6 It is possible that on rare occasions, officers may need to carry out covert surveillance which falls outside the scope of RIPA, either because it falls outside of the Council's core functions (i.e. its specific public functions) and is therefore an ordinary function undertaken by all authorities (e.g., disciplinary investigations) or because the matter under investigation does not pass the imprisonable crime threshold. Such surveillance may not be unlawful, but would take place without the protection afforded by RIPA. In these situations, officers would normally be expected to use similar procedures and forms to those used for RIPA operations, applying the same tests of necessity and proportionality, in order to protect the Council from allegations that it has acted unfairly. Should you wish to conduct such covert surveillance, advice must first be sought from Legal Services.

4 CCTV

4.1 The Council operates a close circuit television system within certain towns in the New Forest District. Use of this system by the council or third parties such as the police for directed surveillance would require authorisation under RIPA.

4.2 Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring traffic flow or public safety will not generally require RIPA authorisation, since the public will be aware that such systems are in use. However, there may be occasions when the Council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required.

4.3 For example, authorisation for directed covert surveillance is likely to be required if the Council wishes to make use of permanently sited overt CCTV cameras in circumstances where Officers have received reports of unlawful trading at a specific location, and wish to use those existing CCTV systems to keep watch for such activities.

4.4 If another agency – eg the Police – wishes to use the Council's CCTV cameras for one of their investigations, this must be agreed by the Head of Public Health and Community Safety, or by the Civil Contingencies and CCTV Manager. A copy of the other agency's RIPA authorisation form must be obtained and the details held with the Council's central register. In such circumstances, as long as there is a Police RIPA authorisation, there is no separate need for one of the Council's Authorised Officers to authorise the use of the cameras.

4.5 **Deployable CCTV**

The deployment of mobile surveillance cameras is likely to be directed surveillance in all cases and appropriate RIPA authorisation will be required. Additionally, applicants will be required to complete a "Mobile CCTV Deployment Form", in accordance with the Council's Deployable (Mobile) CCTV Camera Policy. This form should be submitted to the Council's CCTV Manager.

5 PRIVATE INFORMATION

5.1 The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationships with others, including family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and addresses.

5.2 Whilst a person may have a reduced expectation of privacy when in a public place, surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public. For example, two people holding a conversation on a public street or bus may have a reasonable expectation of privacy, even though they are in a public place.

5.3 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. For example, where an officer drives past a restaurant to take a photograph of the exterior, this is unlikely to require authorisation under RIPA, as the officer is not collecting private information. However, if the officer wishes to revisit the restaurant on a number of occasions to try to establish occupancy of the premises, this is likely to result in the obtaining of private information about the occupier, and authorisation for directed surveillance will usually be required.

6 CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

6.1 This paragraph should be read in conjunction with the Home Office Revised Code of Practice "Covert Human Intelligence Sources" which can be found at https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

6.2 The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person **or**
- To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

A person who uses a relationship to obtain information which they then pass to the Council could be a CHIS, even if the Council hasn't asked them to use their relationship in this way (see paragraph 6.5 below).

6.3 The conduct or use of a CHIS may be authorised under RIPA where it is **necessary** for the **prevention or detection of crime**, or **for the prevention of disorder.**

6.4 A relationship is established or maintained for a covert purpose if it is conducted in a manner to ensure that one of the parties is unaware of its purpose. A relationship will only be used covertly and information will only be disclosed covertly if it is used or disclosed in a way which will ensure that one of the parties is unaware of the use or disclosure.

6.5 The use of such sources by the Council is essentially the manipulation of a relationship to gain information and can amount to the use of an informant.. It should be noted that the use or conduct of a CHIS is a particularly intrusive and high risk covert technique. Therefore, where the use of a CHIS is envisioned there should be sufficient resources dedicated to the oversight and management of the operation. The Council is only likely to use a CHIS in very exceptional circumstances.

6.6 The CHIS will be the person who establishes or maintains the relationship as set out in paragraph 6.2 above.

- The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the Council that is within their personal knowledge, without being induced, asked or tasked by the Council. Therefore, the public can continue to provide information as part of their normal civic duties, or to contact numbers set up by the Council to receive information.

- However, a member of the public providing information **may** be a CHIS if their information is obtained in the course of, or as a consequence of, the existence of a personal or other relationship and they covertly pass that information to the Council. For example, where a member of the public gives repeat information about a suspect and it becomes apparent that the member of the public may be obtaining that information in the course of a family or neighbourhood relationship, it should be considered by the Investigating Officer whether that person is in reality a CHIS.

- This is known as a “status drift”. The Council accordingly needs to be alert to the fact that a public informant may in reality be a CHIS even if not tasked to obtain information covertly.

- Where such a “status drift” occurs, advice must be sought from Legal Services before any information received from this member of the public is relied on.

6.7 **Examples**

6.7.1 The following **will not** be a CHIS:

- A member of the public volunteers a piece of information to the Council regarding something he has witnessed in his neighbourhood. He will not be a CHIS as he is not passing on information as a result of a relationship which has been established or maintained for a covert purpose.
- A person complains about excessive noise coming from their neighbour’s house and the Council ask them to keep a noise diary. They will not be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose.

6.7.2 The following **will** be a CHIS:

- Intelligence received by the Council suggests that a local public house will sell alcohol to minors if they are familiar with them. A person under the age of 18 is engaged and trained by the Council and deployed to attend the licensed premises on a number of occasions and then try and purchase alcohol. In this situation a relationship has been established and maintained for the covert purpose and therefore a CHIS authorisation will be required.
- Without being asked, a person provides regular information to the Council about their neighbours' working hours and income as they believe their neighbour is committing benefit fraud. The person regularly visits their neighbour and engages in conversations about their work for the purpose of obtaining this information and passing it to the Council.

6.8 If a CHIS is used, both the use of the CHIS and their conduct require prior authorisation.

- **Conduct** is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- **Use** includes actions inducing, asking or assisting a person to act as a CHIS.

6.9 The Investigating Officer should apply for such authorisation as soon as the conduct or use of a CHIS is contemplated (see paragraphs 8,9 & 10 below, regarding authorisations and applications).

6.10 **Handling and Controlling the CHIS**

6.10.1 If an authorisation is provided the Investigating Officer must ensure that they are aware of the extent and limits of what the CHIS is allowed to do and make sure that the CHIS is advised of this.

6.10.2 The Investigating Officer will be responsible for the day to day handling of the CHIS (they will be the "handler"). This will involve dealing with the CHIS on behalf of the Council, directing the day to day activities of the CHIS, recording information supplied by the CHIS and monitoring the CHIS's security and welfare.

6.10.3 The safety and welfare of a CHIS both during the operation and after the authorisation has been cancelled should be taken into account by the investigating officer. Every application for authorisation should therefore include a detailed risk assessment of the risk to the CHIS and the likely consequences should the role of the CHIS become known.

6.10.4 The line manager of the "handler" will be the CHIS "controller" and they will be responsible for the management and supervision of the "handler" and the general oversight of the use of the CHIS.

6.10.5 A record must also be made of the use made of the CHIS (see paragraph 17 below for the information which must be held in the Central Log).

6.11 **Records**

Records of relevant documentation relating to every CHIS should be kept for a period of at least five years in accordance with paragraph 17 of this Policy.

6.12 **Special considerations**

6.12.1 Special care should be taken where the use of CHIS may involve confidential information (see paragraphs 2.1 & 11).

6.12.2 Special safeguards should be put in place where the CHIS is under the age of 18. A child under the age of 16 may not be authorised to give information against his parents. The Regulation of Investigatory Powers (Juveniles) Order 2000 contains the special provisions which should be followed where the CHIS is a minor. In such cases the only Authorising Officer is the Chief Executive (or in his absence an Executive Head).

6.12.3 Special safeguards should also be used where the CHIS is a vulnerable individual. A vulnerable individual is defined by the Code of Practice as “a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.” The use of a vulnerable individual is only permitted in exceptional circumstances. In such cases the only Authorising Officer is the Chief Executive (or in his absence an Executive Head).

7 ONLINE COVERT ACTIVITY

7.1 The extent of the information that is now available online, presents new opportunities to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public.

7.2 It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual’s online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

7.3 The use of the internet (including social and business networking sites) may be required to gather information prior to and/or during an operation (including a CHIS operation). This may amount to directed surveillance.

7.4 In addition, a CHIS may communicate online.

7.5 Even if something is posted on a publicly-accessible networking site, it may still be private information. Where the use of the internet is intended as part of an investigation, the investigating officer must consider whether the proposed activity is likely to interfere with a person’s Article 8 right to private and family life. The potential for collateral intrusion should also be considered. Such activity should only be contemplated if it is necessary and proportionate to the specific operation. If private

information is likely to be obtained a directed surveillance authorisation must be obtained.

7.6 Advice should be sought from Legal Services on the use of the internet as part of an investigation.

8 AUTHORISATIONS, RENEWALS, REVIEWS AND CANCELLATIONS

8.1 Prior authorisation is required for the use of **directed surveillance** or the **conduct or use of a CHIS**.

8.2 Procedure for Authorisations

8.2.1 Each officer who undertakes investigations on behalf of the Council must seek authorisation in **writing** for any directed surveillance or the conduct and use of a CHIS.

8.2.2 A full list of Authorising Officers, is shown at **Appendix 1.** Authorising Officers **must not** delegate their powers under RIPA.

8.2.3 A checklist for the respective duties of the Investigating Officer and the Authorising Officer is set out in **Appendix 2.** Further detail is provided on some of these duties in this Policy.

8.2.4 All applications for authorisations should be made on the applicable standard form (See paragraph 9).

8.2.5 The Authorising Officer must describe explicitly in the authorisation what is being authorised. This should be in the Authorising Officer's own words rather than merely by reference to the terms of the application.

8.2.6 The Authorising Officer may add a proposed activity to the application if it is deemed necessary, and the Authorising Officer may authorise only some of what is being requested by the Investigating Officer. Where only part of the application is being authorised, the Authorising Officer should state the reason for this decision.

8.2.7 Authorising Officers should not normally be responsible for authorising operations in which they are directly involved as the Authorising Officer should be independent of the investigations. Where this is unavoidable this must be highlighted on the authorisation.

8.2.8 Every authorisation must state the rank of the person providing it.

8.3 Authorisations Requiring Judicial Approval

8.3.1 Since **1 November 2012**, where an authorisation has been granted for directed surveillance or the conduct or use of a CHIS, that authorisation shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court. **No directed surveillance or the use of a CHIS can take place until this approval has been obtained.**

8.3.2 Legal Services should be instructed to prepare the application to the justice of the peace.

8.4 **Duration**

8.4.1 The time limit for a standard **written** authorisation for directed surveillance is 3 months from the day of the authorisation.

8.4.2 The time limit for a standard **written** authorisation for a CHIS is 12 months from the day of the authorisation.

8.4.3 It should be noted that even if an authorisation is only required for a limited time, it must still be for the statutory periods outlined above. However, the authorisation can be reviewed and/or cancelled if it is no longer necessary and proportionate.

8.4.4 No further operations can be carried out after the expiry of the relevant authorisation unless it has been renewed.

8.4.5 It will be the responsibility of the Investigating Officer to ensure that direct surveillance or the conduct or use a CHIS is only undertaken under an appropriate and valid authorisation. It will be the Investigating Officer's responsibility to diarise when the authorisation expires.

8.5 **Reviews**

8.5.1 The Authorising Officer will be responsible for reviewing each authorisation at regular intervals. The Authorising Officer shall determine how often a review should take place at the outset and each review should be conducted by the predetermined date. As a guide, reviews should take place on a monthly basis. However, the Authorising Officer may determine that they should take place more or less frequently (if so, the reasons should be recorded).

8.5.2 Reviews should take place as often as necessary and practicable and this will need to be determined on a case by case basis. More frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information. (see paragraphs 2.1, 2.2 & 11).

8.5.3 Reviews should also be held in response to changing circumstances and must take into account any subsequent action by the Council arising from the product of the surveillance, which may be in the form of the issue of notices, orders, or determinations by the Council, or the bringing of criminal or civil proceedings, or any other action.

8.5.4 It will be the responsibility of the Authorising Officer to diarise when reviews should be held.

8.5.5 All reviews should be recorded on the correct form (See paragraph 9).

8.6 **Renewal**

8.6.1 An authorisation may be renewed **before** it ceases to have effect if an Authorising Officer considers it necessary for the authorisation to continue. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary a renewal can be made more than once.

8.6.2 Before a renewal of an authorisation for the conduct or use of a CHIS the Authorising Officer must be satisfied that a review has taken place of:

- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation; and
- the tasks given to the source during that period and the information obtained from the conduct or the use of the source.

8.6.3 Since **1 November 2012**, where renewal of an authorisation has been granted for directed surveillance or a CHIS that renewal shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court.

8.6.4 Where the renewal relates to the conduct or use of a CHIS the Justice of the Peace will need to be satisfied that a review has taken place of the matters listed in paragraph 7.6.2.

8.6.5 All renewals must be made on the correct form. (See paragraph 9).

8.7 **Cancellations**

8.7.1 All authorisations must be cancelled **as soon as** they are no longer required.

8.7.2 Even if an authorisation has expired it will not lapse and should be formally cancelled.

8.7.3 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply e.g. the aims have been met; risks have changed and authorisation is no longer appropriate.

8.7.4 If the Authorising Officer is not available, this duty will fall on one of the other Authorising Officers.

8.7.5 When cancelling an authorisation, the Authorising Officer should (where applicable):

- Record the date and times (if at all) that surveillance took place, and that the order to cease the activity was made.
- Record reason for the cancellation.
- Ensure that surveillance equipment has been removed and returned.
- Provide directions for the management of the material obtained as a result of the investigation.
- Ensure that the detail of persons subjected to surveillance since the last review or renewal is properly recorded.
- Record the value of the surveillance and interference (i.e. whether the objectives as set out in the authorisation were met.)

8.7.6 Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed and recorded on the central record of authorisations. However, best practice will be for the authorisation to be cancelled in writing.

8.7.7 The Authorising Officer should also advise those involved in the surveillance or the CHIS to stop their actions with immediate effect.

8.7.8 Where necessary, when cancelling the use of a CHIS, the Authorising Officer should consider the safety and welfare of the CHIS, and should satisfy themselves that all safety and welfare matters are addressed.

8.7.9 All cancellations must be completed on the correct form (See paragraph 9).

9 APPLICATION FORMS

9.1 The standard forms can be found at https://www.gov.uk/government/collections/ripa-forms--2

9.2 The person completing the form is responsible for ensuring that the form used is the most up-to-date version issued by the Governement.

9.3 The forms for applications, renewals, reviews and cancellations should be completed in as much detail as possible.

9.4 For guidance on what should be included in the application for authorisation the Investigating Officer should refer to paragraph 5.6 of the 2018 Covert Surveillance and Property Interference Revised Code of Practice (for direct surveillance) or paragraph 5.11 in the 2018 Covert Human Intelligence Sources Revised Code of Practice (for CHIS).

9.5 Each investigation or operation should be given a unique reference number ("URN") on the application form by the Legal Services Manager. Any reviews, renewals or cancellation forms should be identified by the same URN.

9.6 The URN should be obtained from the Legal Services Manager (see paragraph 18).

9.7 Any application (or other) form which is not completed in full will be rejected by the Authorising Officer.

9.8 The role of the Investigating Officer is to present the facts and evidence to the Authorising Officer. They must also set out in detail why they consider the directed surveillance/use of a CHIS to be **necessary** and **proportionate** (see paragraph 10). The application should include consideration of any potential collateral intrusion (see paragraph 2.2) and measures taken to limit this. The application must state whether the Investigating Officer expects the investigation to result in the obtaining of confidential information (see paragraphs 2.1 &11).

9.9 Having reviewed the application, the Authorising Officer must decide whether they consider the activities applied for are **necessary** and **proportionate** (see paragraph 10). If so, they should decide whether to authorise some or all of the activities applied for. If they decide to authorise the application, they must record in detail the reasons that they have reached this decision, including the reasons that they have concluded the activities are necessary and proportionate.

10 THE NECESSITY AND PROPORTIONALITY TEST

10.1 No directed surveillance or use of a CHIS can be authorised under RIPA unless it can be demonstrated that it is necessary and proportionate.

10.2 The Authorising Officer must be satisfied that the proposed surveillance is **necessary and proportionate**.

10.3 **Necessary**

10.3.1 The use of the directed surveillance or conduct and use of a CHIS must be **necessary** for the **purpose of preventing or detecting crime** or **of preventing disorder**.

10.3.2 In order for the Authorising Officer to be satisfied that the surveillance is necessary, the Investigating Officer must clearly identify in the application the conduct that it is aimed to prevent or detect, and an explanation of why covert techniques are required.

10.4 **Proportionate**

10.4.1 The intrusion into the private and family life of the subject of the operation must be **balanced** against what the activity seeks to achieve. The intrusion must not be excessive or arbitrary.

10.4.2 The authorisation should therefore demonstrate how the Authorising Officer reached the conclusion that the act is proportionate

10.4.3 The activities will not be proportionate if the activities are excessive in the circumstances of the case or if the information could be obtained by a less intrusive means.

10.4.4 The following elements of proportionality must be considered by the Authorising Officer and should be addressed in the authorisation:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

10.4.5 When authorising a CHIS, the Authorising Officer must also:

- be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
- be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
- consider the likely degree of intrusion for all those potentially affected;
- consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and
- ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

10.4.6 **Risk of Collateral Intrusion**

The Authorising Officer should consider the likely effect of the use of the direct surveillance or the conduct and use of a CHIS on the private and family life of persons who are not the intended subjects of the activity. The Authorising Officer must consider the risk of collateral intrusion and have a plan for managing any such risk.

If the impact on other persons cannot be avoided altogether, then any collateral intrusion must be proportionate.

The person carrying out the surveillance must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation ought to continue or whether a new authorisation is required.

11 CONFIDENTIAL MATERIAL

11.1 Particular care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy and where it is envisaged that the investigation may cause the Council to come into possession of Confidential Information (see definition at paragraph 2.1). In these cases, the surveillance can only be authorised by the Chief Executive (or in his absence an Executive Head). Applications which are calculated to obtain confidential information will only be authorised in very exceptional and compelling circumstances.

11.2 Where an Investigating Officer comes into possession of confidential material during the course of an investigation, s/he should seek legal advice from a member of the Council's Legal Services before taking any action in connection with that material.

11.3 Where it is envisaged that surveillance may cause the Council to come into possession of material which is subject to legal privilege, the Investigating Officer must seek legal advice from a member of the Council's Legal Services Section before the application for authorisation is made.

12 ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The Investigating Officer must make enquiries of other public authorities whether they are carrying out similar activities, if he considers that there is such a possibility, in order to ensure that there is no conflict between the activities of the Council and those other public authorities.

13 JOINT INVESTIGATIONS

13.1 From time to time, Council officers may carry out investigations with officers from another public authority, for example:

- The police;
- The Department of Work and Pensions;
- The Environment Agency;
- The Food Standards Agency; or
- The Health and Safety Executive

13.2 Where one authority is acting on behalf of another, the tasking authority should normally obtain the RIPA authorisation. If an authorisation has been obtained by another agency, who wish the Council to carry out surveillance in accordance with that authorisation, an Authorising Officer must view that authorisation to ensure that Council officers, and the activities which they are being asked to carry out, are covered by that authorisation.

14 DATA PROTECTION

Private information collected as a result of surveillance may include personal data. It is the responsibility of the Authorising Officer to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the General Data Protection Regulation, the Data Protection Act 2018 and the Council's Data Protection Policy, Law Enforcement (Data Protection) Policy and the Protection of Special Category Data Policy.

15 DESTRUCTION OF WHOLLY UNRELATED MATERIAL

15.1 Surveillance may result in officers obtaining the following categories of material:

i. material which is wholly unrelated to the investigation (for example, information about persons who are not the subject of the surveillance, and have no relevant involvement with the subject of the surveillance);

ii. material regarding the subject(s) of the surveillance, which is unlikely to be used in connection with the investigation or any subsequent proceedings;

iii. material which is relevant to the investigation, and may be used in connection with subsequent proceedings

15.2 Material which is **wholly unrelated** to the investigation (category **i.** above) should be destroyed promptly and securely. As the material will have been collected in

connection with the investigation of a criminal offence, advice should be sought from the Council's Legal Services section prior to the destruction of evidence.

15.3 All other material should be retained until the investigation is concluded and a decision is taken regarding what action, if any, will be taken in connection with the investigation. At that stage, the Authorising Officer will determine which materials are to be retained, and for how long.

15.4 Where criminal proceedings are contemplated, all material (save for wholly unrelated material) is potentially relevant. It must therefore be retained and will be disclosable in those proceedings.

16 TRAINING

16.1 Each officer of the Council with responsibilities for the conduct of an investigation, operation or authorisation under RIPA, will undertake training every three years to ensure that any such investigations, operations and authorisations undertaken are conducted according to the statutory requirements and the Codes of Practice. However, where a RIPA investigation is contemplated, the relevant officers are required to contact Legal Services in advance so an update training session can be provided.

16.2 Each officer who undertakes training in connection with their responsibilities under RIPA must keep a personal training record, and must send a copy of this training record every two years to the Legal Services Manager.

17 RECORDS OF AUTHORISATIONS

17.1 A centrally retrievable record of all authorisations will be held by the Legal Services Manager. This will contain the following information:

- the type of authorisation
- the URN
- the dates that the authorisation was granted, reviewed, renewed or cancelled.
- details of attendances at the Magistrates' Court to include date of attendances, the determining Magistrate, the decision of the Court and the time and date of that decision.
- the name and rank of the Authorising Officer for the initial authorisation and any reviews, renewals or cancellations.
- whether the Authorising Officer is involved in the investigation.
- the file reference for the investigation.
- whether the authorisation was likely to result in the obtaining of confidential material.

17.2 This centrally retrievable record will be stored in a manner which is confidential and secure. It will be retained for a period of at least **three years** from the date of

cancellation of the authorisation for directed surveillance, and at least **five years** from the date of cancellation of the authorisation of a CHIS.

17.3 In addition, the Legal Services Manager will keep the following documents, where applicable, for a period of at least **three years** from the date of cancellation of the authorisation for directed surveillance, and at least **five years** from the date of cancellation of the authorisation of a CHIS:

- The application, authorisation, reviews, renewals, cancellations and the approval from the Magistrates Court.
- The frequency of the reviews prescribed by the authorising officer.
- The date and time when any instruction to cease directed surveillance or use of a CHIS was given.
- The date and time when any other instruction was given by an Authorising Officer.

17.4 In relation to the use of a CHIS the Legal Services Manager will also maintain the following documents:

- Any risk assessment in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.

17.5 Investigating Officers and Authorising Officers may keep copies of relevant documentation but any such copies should be stored in a manner which is confidential and secure.

18 MONITORING

18.1 The Legal Services Manager will have responsibility for overseeing the authorising process to ensure good quality control of RIPA and will be referred to as the Legal Services Manager for the purposes of this Policy (see **Appendix 3**).

18.2 The Legal Services Manager will be responsible, along with the Senior Responsible Officer, for ensuring corporate awareness of RIPA.

18.3 The Legal Services Manager will be responsible for issuing each application with a URN.

18.4 All completed RIPA forms; applications (whether granted or refused), authorisations, reviews, renewals and cancellations, and approvals from the Magistrates' Court should be forwarded to the Legal Services Manager within **five working days** of the relevant decision. The Legal Services Manager will hold these documents securely.

18.5 The Legal Services Manager will also be responsible for the day to day management of the authorising process, and any initial queries from Investigating Officers or Authorising Officers should be addressed to the Legal Services Section.

18.6 Adherence to the requirements of RIPA, the Codes of Practice and this Policy should reduce the scope for making errors. The Legal Services Manager will conduct a regular review of errors and a record must be made of each review.

19 SENIOR RESPONSIBLE OFFICER

19.1 The Senior Responsible Officer will be the Chief Executive (see **Appendix 3**).

19.2 The Senor Responsible Officer will be responsible for the following:

- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance.
- Compliance with RIPA and with the Codes of Practice.
- Ensuring all Authorising Officers are of an appropriate standard.
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable.
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

20 POLICY AND IMPLEMENTATION

20.1 The Policy is operational from **15 January 2019** and replaces any previous policies and procedures relating to surveillance.

20.2 The Legal Services Manager will report annually to the Audit Committee regarding the use made by the Council of its powers under RIPA.

20.3 The Audit Committee will review the Council's Surveillance Policy annually.

21 APPENDICES

Appendix 1 – Functions that may be undertaken by Authorising Officers

Appendix 2 - Application and Authorisation Checklist

Appendix 3 – Monitoring and Senior Responsible Officers

APPENDIX 1

FUNCTIONS THAT MAY BE UNDERTAKEN BY AUTHORISING OFFICERS:

1. Authorise an **application** for authority to carry out directed surveillance or for the conduct or the use of a CHIS.

2. **Review** an authorisation to carry out directed surveillance or the conduct or use of a CHIS on or before the specified date.

3. Authorise **renewal** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

4. Authorise **cancellation** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

5. Authorise **destruction** of wholly unrelated material arising from surveillance or from the conduct or use of a CHIS, with advice from the Legal Services Section where appropriate.

6. **Monitor** the produce of the surveillance or from the conduct or use of a CHIS.

7. Authorise an application where the likely consequence of directed surveillance or conduct or use of a CHIS would be intrusion on another person other than the target **(collateral Intrusion).**

8. Authorise an application where the likely consequence of the directed surveillance or conduct or use of a CHIS would result in Council obtaining **confidential material.**

9. Authorise the use of a CHIS who is a minor.

10. Authorise the use of a CHIS who is a vulnerable person.

RANK/TITLE	**AUTHORISED FUNCTIONS**
Chief Executive	1-10
Executive Heads	1-7 (8,9,10 in Chief Executive's absence)
Service Managers for: Planning Environmental and Regulation Street Scene Revenue and Benefits Housing Estates Management & Support.	1-7

APPENDIX 2

APPLICATION AND AUTHORISATION CHECKLIST

Investigating Officer must:

Read the Surveillance Policy document and be aware of any other relevant guidance.	
Determine that directed surveillance and/or a CHIS is required.	
For directed surveillance , assess whether the authorisation will be in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and be able to demonstrate that the suspected offence is subject to a custodial sentence of 6 months or more or that the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.	
Consider whether surveillance will be proportionate.	
Consider all less intrusive options which may be available and practicable **and use that option first.**	
If authorisation is **necessary and proportionate**, request a URN from the Legal Services Manager, prepare and submit an application to carry out directed surveillance or conduct or use of a CHIS to an Authorising Officer.	
REVIEW REGULARLY and submit to Authorising Officer on date set.	
If operation is no longer necessary or proportionate, complete **cancellation form** and submit to Authorising Officer.	

Authorising Officer must:

Consider in detail whether all options have been duly considered, including taking into account the Surveillance Policy document and any other relevant guidance.	

For directed surveillance, confirm that the offence is subject to a custodial sentence of 6 months or more or the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Consider whether surveillance can be considered to be in accordance with the law and is **necessary and proportionate** to the offence being investigated.	
Authorise **only** if an overt or less intrusive option is not practicable.	
Ensure the relevant judicial authority has made an order approving the grant of the authorisation.	
If surveillance is necessary and proportionate: • Review authorisation • Set review timetable (at least monthly)	
Cancel authorisation when it is no longer necessary or proportionate.	

ESSENTIAL:

- Officers must use the correct RIPA forms (which can be found on the Home Office website www.homeoffice.gov.uk).
- A URN must be obtained from the Legal Services Manager before submitting an application for authorisation.
- Once authorised, approval must be obtained from a Magistrates Court before any surveillance commences.
- All RIPA application forms (whether authorised or rejected) must be sent to the Legal Services Manager **within 5 working days**. This must include reviews, renewals and cancellations
- If in any doubt, seek advice from the Legal Services Manager or the Senior Responsible Officer **before** any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

APPENDIX 3

MONITORING AND SENIOR RESPONSIBLE OFFICERS

Name	Job Title	RIPA Role
Bob Jackson	Chief Executive	Senior Responsible Officer
Andrew Kinghorn	Legal Services Manager	Monitoring